

DIGITAL DATA RECORDER WITH SECURITY INFORMATION

Publication number: JP2000056681

Publication date: 2000-02-25

Inventor: IIZUKA NORIO

Applicant: CASIO COMPUTER CO LTD

Classification:

- International: G06F12/14; G06F21/24; G09C1/00; G09C5/00;
H04N1/44; G06F12/14; G06F21/00; G09C1/00;
G09C5/00; H04N1/44; (IPC1-7): G09C1/00; G06F12/14;
G09C1/00; G09C5/00; H04N1/44

- European:

Application number: JP19980236342 19980807

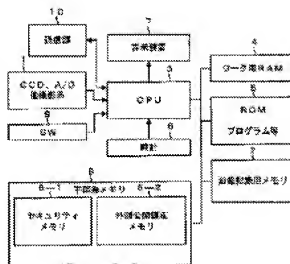
Priority number(s): JP19980236342 19980807

Report a data error here

Abstract of JP2000056681

PROBLEM TO BE SOLVED: To provide a digital data recorder with security information which prevents digital data from being falsified, reproduced, partially used, or illegally used.

SOLUTION: A CPU 3 generates a public key and a secret key by a public key cryptosystem. Then, an ID image stored in a security memory 8-1 is used as a random number series source. Moreover, the CPU 3 appends additional information to the image data inputted from a pickup system 1, and encodes the data with the secret key, to generate an electronic signature data. Further, the CPU summarizes the input data main body to which the additional information is appended, the electronic signature data, and the public key, etc., and generates a data file. In the case of restoring the data file, if the data acquired by decoding the electronic signature data by using the public key appended to the data file coincides with the data acquired from the main body of the data file, it can be judged that neither falsification nor edit, etc., are added thereto.

Data supplied from the [esp@cenet](http://www.esp@cenet.com) database - Worldwide

(51) Int.Cl. ⁷	識別記号	F I	デコード [*] (参考)
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 Z 5 B 0 1 7
	6 4 0		6 4 0 B 5 C 0 7 5
	6 6 0		6 6 0 D
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 A
G 0 9 C 5/00		G 0 9 C 5/00	

審査請求 未請求 請求項の数16 F D (全 17 頁) 最終頁に続く

(21) 出願番号 特願平10-236342

(22) 出願日 平成10年8月7日 (1998.8.7)

(71) 出願人 000001443

カシオ計算機株式会社
東京都渋谷区本町1丁目6番2号

(72) 発明者 飯塚 宜男

東京都羽村市栄町3丁目2番1号 カシオ
計算機株式会社羽村技術センター内

(74) 代理人 100096099

弁理士 鹿嶋 実貴

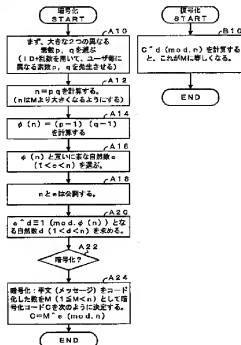
Fターム(参考) 5B017 AA06 AA07 BA05 BA07 BA09
BB02 BB07 CA12 CA16
5C075 CA14 CD05 CD07 ED02 ED03
FF90

(54) 【発明の名称】 セキュリティ情報付きデジタルデータ記録装置

(57) 【要約】

【課題】 デジタルデータの改竄や複製、部分使用、不正使用を防止できるセキュリティ情報付きデジタルデータ記録装置を提供する。

【解決手段】 CPU 3は、公開鍵暗号方式により公開鍵および秘密鍵を生成する。このとき、セキュリティメモリ8-1に格納されているID画像を乱数系列発生源として用いる。また、CPU 3は、撮影系1から入力された画像データに付加情報を添付し、該データを上記秘密鍵により暗号化し、電子署名データを生成する。さらに、上記付加情報が添付された入力データ本体、電子署名データ、上記公開鍵等をまとめ、データファイルを生成する。該データファイルを復元する際には、データファイルに添付されている公開鍵を用いて電子署名データを復号化して取得したデータと、データファイルのデータ本体から取得したデータとが一致すれば、改竄、複製等が加えられていないと判断できる。



【特許請求の範囲】

【請求項1】 公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、 デジタルデータを入力する入力手段と、

前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、

前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、

前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、

前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する閲覧ファイル生成手段とを具備することを特徴とするセキュリティ情報付きデジタルデータ記録装置。

【請求項2】 前記閲覧ファイルに付加されている公開鍵により、閲覧ファイルに添付されている電子署名データを復号化する復号化手段と、

前記閲覧ファイルに添付されている入力データ本体と前記復号化手段により復元されたデータとを比較し、双方が一致した場合には、入力データ本体が改竄されていないと判断し、双方が一致しない場合には、入力データ本体が改竄されていると判断する判断手段と 前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記判断手段による判断結果を表示する表示手段とを具備することを特徴とする請求項1記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項3】 前記入力データ本体が暗号化される前段で、入力データ本体から特徴データを抽出し、ダイジェスト化する特徴データ抽出手段を具備し、前記電子署名名手段は、前記特徴データ抽出手段によりダイジェスト化されたデータを、前記鍵生成手段により生成された秘密鍵により暗号化し、電子署名データを生成することを特徴とする請求項1記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項4】 前記鍵生成手段は、デジタルデータの記録を識別するための識別データに基づいて、公開鍵および秘密鍵を生成することを特徴とする請求項1記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項5】 前記識別データは、デジタルデータの記録者が選択した任意の識別画像データであることを特徴とする請求項4記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項6】 前記識別画像データを所定のサイズに間引く間引き手段を具備し、

前記付加情報生成手段は、前記間引き手段により間引かれた識別画像データを前記入力手段から入力されたデジ

タルデータに付加情報として添付することを特徴とする請求項5記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項7】 配信相手毎に、配信相手を選定する識別情報として、配信相手によって予め設定された識別画像データを記憶する配信相手情報記憶手段と、前記配信相手情報記憶手段に記憶されている識別画像データを指定することで、前記閲覧ファイル生成手段により生成された閲覧ファイルの配信相手を選択する配信先選択手段とを具備することを特徴とする請求項1記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項8】 配信相手毎に、配信相手を選定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを記憶する配信相手情報記憶手段と、

前記電子署名生成手段により生成された電子署名データを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段を具備し、前記閲覧ファイル生成手段は、前記暗号化手段により暗号化された暗号データおよび公開可能な公開情報をまとめ、閲覧ファイルを生成することを特徴とする請求項1記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項9】 前記公開情報は、少なくとも、公開可能な画像データを含むことを特徴とする請求項8記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項10】 前記閲覧ファイルを自身の秘密鍵により復号化する第2の復号化手段と、前記復号化手段は、前記第2の復号化手段により復元されたデータに添付されている公開鍵により、復元されたデータに添付されている電子署名データを復号化することを特徴とする請求項9記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項11】 前記判断手段は、前記第2の復号化手段による復元が失敗した場合には、前記閲覧ファイルが不正に入手されたと判断し、

前記表示手段は、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記公開情報に含まれる公開可能な画像データを表示することを特徴とする請求項10記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項12】 前記公開情報は、閲覧ファイルに添付されているデータ本体が暗号化ファイル、電子署名付きファイル、セキュリティ情報なしファイルのいずれであるかを示すファイル種別情報を含むことを特徴とする請求項11ないし1記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項13】 前記電子署名手段による電子署名データの生成に先立って、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込む電子透かし手段を具備

することを特徴とする請求項1記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項14】 前記判断手段は、前記閲覧ファイルに付加されている公開鍵と、前記閲覧ファイルのデータ本体に電子透かし情報として入れ込まれた公開鍵とを比較し、双方が一致した場合には、入力データ本体が正当な配信者からのデータであると判断することを特徴とする請求項13記載のセキュリティ情報付きデジタルデータ記録装置。

【請求項15】 公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、配信相手毎に、配信相手特定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを記憶する配信相手情報記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名データにより生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する第1の閲覧ファイル生成手段と、前記第1の閲覧ファイル生成手段により生成された閲覧ファイルを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段と、ファイル本体の種別を示すファイル種別情報、前記暗号化手段により暗号化された暗号データ、および公開可能な公開画像データをまとめ、特定の相手に対する閲覧ファイルの生成する第2の閲覧ファイル生成手段とを具備することを特徴とするセキュリティ情報付きデジタルデータ記録装置。

【請求項16】 公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込む電子透かし手段と、前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記電子透かし手段により電子透かしが施されたデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記

憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生成する閲覧ファイル生成手段とを具備することを特徴とするセキュリティ情報付きデジタルデータ記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子スチルカメラ等のデジタルデータ記録装置に係り、記録したデジタルデータの閲覧・配信に際し、セキュリティ向上を図るセキュリティ情報付きデジタルデータ記録装置に関する。

【0002】

【従来の技術】電子スチルカメラ等の入力/デジタル変換機器は、パソコンとの装置との接続、転送のしやすさから、著作物的な意味合いや、業務上の記録、証拠などに用いることができるが、デジタルデータであるがゆえに、編集、改竄を比較的自由に行うことができる。

【0003】一方、通信や当事者間の通信のセキュリティのために、当事者間の秘密通信や、内容証明通信のために、公開鍵方式や、共有鍵方式を応用した暗号化および電子署名の主々の方式や、不正複製や一部流用の検出/抑制のため、特に著作権情報等を入れ込むための、電子透かしなどの処理がある。

【0004】これら既存の方式により、パソコンに取り込んだ画像や音声、動画データに対して、セキュリティに対する対策を施すことは可能である。しかし、これらは、パソコン上の処理プログラムになっており、生データである画像や音声のファイルの記録/生成時には、保証する方法がなかった。

【0005】

【発明が解決しようとする課題】したがって、デジタル画像データ等の生データファイルについては、当事者間の秘密通信においても、また、インターネットのWeb公開等で、デジタル署名を付加して内容保証をしたデータであらうと、電子スチルカメラ>PCの経路において、および、撮影した瞬間の、保証ができていないため、不正入手した画像をパソコンに取り込んだ時点で、保証データを付加した否かは判定することができなかった。

【0006】また、業務において、デジタル画像等を用いる場合にも、改竄を防止するなど、データの正当性が証明されなくてはならず、これは、生データ撮影時(作成時)に付加されるものでなければ、セキュリティ的にもユーザの使い勝手としても、問題であった。また、電子透かしにおいても、撮影した画像がそのまゝ著作物として利用されることを考えると、データの作成時に情報を入れ込めないで、同様の問題があった。

【0007】そこで本発明は、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるセキュリティ情報付きデジタルデータ記録装置を提供することを目的とする。

【0008】

【課題を解決するための手段】上記目的達成のため、請求項1記載の発明によるセキュリティ情報付きデジタルデータ記録装置は、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめ、閲覧ファイルを生産する閲覧ファイル生成手段とを具備することを特徴とする。

【0009】また、好ましい態様として、例えば請求項2記載のように、請求項1記載のセキュリティ情報付きデジタルデータ記録装置において、前記閲覧ファイルに付加されている公開鍵により、閲覧ファイルに添付されている電子署名データを復号化する復号化手段と、前記閲覧ファイルに添付されている入力データ本体と前記復号化手段により復元されたデータとを比較し、双方が一致した場合には、入力データ本体が改竄されていないと判断し、双方が一致しない場合には、入力データ本体が改竄されていると判断する判断手段と前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記判断手段による判断結果を表示する表示手段とを具備することを特徴とする。

【0010】また、好ましい態様として、例えば請求項3記載のように、請求項1記載のセキュリティ情報付きデジタルデータ記録装置において、前記入力データ本体が暗号化される前段で、入力データ本体から特徴データを抽出し、ダイジェスト化する特徴データ抽出手段を具備し、前記電子署名手段は、前記特徴データ抽出手段によりダイジェスト化されたデータを、前記鍵生成手段により生成された秘密鍵により暗号化し、電子署名データを生成することを特徴とする。

【0011】また、好ましい態様として、例えば請求項4記載のように、請求項1記載のセキュリティ情報付きデジタルデータ記録装置において、前記鍵生成手段は、デジタルデータの記録者を識別するための識別データに基づいて、公開鍵および秘密鍵を生成することを特徴とする。

【0012】また、好ましい態様として、例えば請求項5記載のように、請求項4記載のセキュリティ情報付きデジタルデータ記録装置において、前記識別データは、デジタルデータの記録者が選択した任意の識別画像データであることを特徴とする。

【0013】また、好ましい態様として、例えば請求項6記載のように、請求項5記載のセキュリティ情報付きデジタルデータ記録装置において、前記識別画像データを所定のサイズに開く開き手段を具備し、前記付加情報生成手段は、前記開き手段により開かれた識別画像データを前記入力手段から入力されたデジタルデータに付加情報として添付することを特徴とする。

【0014】また、好ましい態様として、例えば請求項7記載のように、請求項1記載のセキュリティ情報付きデジタルデータ記録装置において、配信相手毎に、配信相手を選定する識別情報として、配信相手によって予め設定された識別画像データを記憶する配信相手情報記憶手段と、前記配信相手情報記憶手段に記憶されている識別画像データを指定することで、前記閲覧ファイル生成手段により生成された閲覧ファイルの配信相手を選択する配信先選択手段とを具備することを特徴とする。

【0015】また、好ましい態様として、例えば請求項8記載のように、請求項1記載のセキュリティ情報付きデジタルデータ記録装置において、配信相手毎に、配信相手を選定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め設定された公開鍵とを記憶する配信相手情報記憶手段と、前記電子署名生成手段により生成された電子署名データを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段を具備し、前記閲覧ファイル生成手段は、前記暗号化手段により暗号化された暗号データおよび公開可能な公開情報をまとめ、閲覧ファイルを生産することを特徴とする。

【0016】また、好ましい態様として、例えば請求項9記載のように、請求項8記載のセキュリティ情報付きデジタルデータ記録装置において、前記公開情報は、少なくとも、公開可能な画像データを含むことを特徴とする。

【0017】また、好ましい態様として、例えば請求項10記載のように、請求項9記載のセキュリティ情報付きデジタルデータ記録装置において、前記閲覧ファイルを自身の秘密鍵により復号化する第2の復号化手段と、前記復号化手段は、前記第2の復号化手段により復号されたデータに添付されている公開鍵により、復元されたデータに添付されている電子署名データを復号化することを特徴とする。

【0018】また、好ましい態様として、例えば請求項11記載のように、請求項10記載のセキュリティ情報付きデジタルデータ記録装置において、前記判断手段は、前記第2の復号化手段による復元が失敗した場合に

は、前記閲覧ファイルが不正に入手されたと判断し、前記表示手段は、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記公開情報に含まれる公開可能な画像データを表示することと特徴とする。

【0019】また、好ましい態様として、例えば請求項12記載のように、請求項1ないし11記載のセキュリティ情報付きデジタルデータ記録装置において、前記公開情報は、閲覧ファイルに添付されているデータ本体が暗号化ファイル、電子署名付きファイル、セキュリティ情報なしファイルのいずれであることを示すファイル種別情報を含むことを特徴とする。

【0020】また、好ましい態様として、例えば請求項13記載のように、請求項1記載のセキュリティ情報付きデジタルデータ記録装置において、前記電子署名手段による電子署名データの生成に先立って、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込む電子透かし手段を具備することを特徴とする。

【0021】また、好ましい態様として、例えば請求項14記載のように、請求項13記載のセキュリティ情報付きデジタルデータ記録装置において、前記判断手段は、前記閲覧ファイルに付加されている公開鍵と、前記閲覧ファイルのデータ本体に電子透かし情報として入れ込まれた公開鍵とを比較し、双方が一致した場合には、入力データ本体が正当な配信者からのデータであると判断することを特徴とする。

【0022】また、上記目的達成のため、請求項15記載の発明によるセキュリティ情報付きデジタルデータ記録装置は、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータに関する付加情報を生成し、前記入力手段から入力されたデジタルデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、配信相手毎に、配信相手と特定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを記憶する配信相手情報記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報とをまとめ、閲覧ファイルを生成する第1の閲覧ファイル生成手段と、前記第1の閲覧ファイル生成手段により生成された閲覧ファイルを、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化する暗号化手段と、ファイル本体の種別を示すファイル種

別情報、前記暗号化手段により暗号化された暗号データ、および公開可能な公開画像データとをまとめ、特定の相手に対する閲覧ファイルを生成する第2の閲覧ファイル生成手段とを具備することを特徴とする。

【0023】また、上記目的達成のため、請求項16記載の発明によるセキュリティ情報付きデジタルデータ記録装置は、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、デジタルデータを入力する入力手段と、前記入力手段から入力されたデジタルデータから入力されたデジタルデータに関する付加情報を生成し、前記電子透かし手段により電子透かしが施されたデータに添付する付加情報生成手段と、前記付加情報生成手段により生成されたデータを入力データ本体として記憶する記憶手段と、前記鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成する電子署名手段と、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報とをまとめ、閲覧ファイルを生成する閲覧ファイル生成手段とを具備することを特徴とする。

【0024】

【発明の実施の形態】まず、実施例に先立ち、本実施例が前提とする公開鍵暗号方式のうち、RSA公開鍵暗号方式について簡単に説明しておく。RSA公開鍵暗号とは、1979年に、MIT（マサチューセッツ工科大学）のRivest, Shamir, Adelmanが提唱した方式である。なお、RSA公開鍵暗号については、米国特許4,405,829号（暗号通信システムと手法）などで述べられている。

【0025】なお、本実施例では、特にRSA暗号でなくとも、公開鍵方式で、暗号化とデジタル署名の両方を行うことのできる暗号化方式なら暗号化方式には制限はない。また、暗号化ファイルのやりとりの機能に限定しただけなら、本実施例とはほとんど同じ態様で、共通鍵方式の暗号（DES、FEALなど）にも対応可能である。ここで、図1は、RSA公開鍵暗号方式を説明するためのフローチャートである。以下、図1のフローチャートを参照してRSA公開鍵暗号方式を説明する。

【0026】まず、暗号化処理においては、ステップA10で、大きな2つの異なる素数 p 、 q を選ぶ。本実施例では、ユーザー毎に特有のIDと乱数とを用いて、ユーザー毎に異なる素数 p 、 q を生成している。次に、ステップA12で、 $n=pq$ を計算する。このとき、 n は、後述するより大きな数となる。次に、ステップA14で、 $\phi(n) = (p-1)(q-1)$ を計算し、ステップA16で、 $\phi(n)$ と互いに素な自然数 e （ $1 <$

$e < n$)を選び、ステップA18で、上記 n と e とを公開する。

【0027】次に、ステップA20で、 $e^{-1}d \equiv 1 \pmod{\phi(n)}$ となる自然数 d ($1 < d < n$)を求める。上記 (n, e) のペアが公開鍵、 d が秘密鍵となる。また、素数 p, q は秘密であり、絶対公開してはならない値である。公開鍵 (n, e) から秘密鍵 d を求めることは困難であることが知られている。そして、ステップS22で、暗号化が否かを判断し、暗号化であれば、ステップA24で、平文(メッセージ)をコード化した数 M ($1 \leq M < n$)として、公開鍵 (e, m) を用いて、 $C = M^e \pmod{n}$ なる演算で暗号コード C を生成する。

【0028】また、復号化処理では、ステップB10で、暗号化されたコード C 、秘密鍵 d 、 e と d の関係により決まる係数 n に従って、 $M = C^d \pmod{n}$ を計算することで、元のメッセージ M を取得する。秘密鍵 d は、受信した相手のみが知っているため、該受信者が復号化できないようになっている。

【0029】なお、本実施形態による公開鍵を用いた暗号化手法には、以下の特徴がある。

〔公開鍵暗号について〕

1. 暗号化鍵と復号化鍵を別のものにする。
2. 暗号化は極めて容易である。
3. 鍵など復号化することは、たとえ仕組みがわかったとしても、事実上不可能である。
4. 暗号化鍵は公開する(公開鍵)。復号化鍵は秘密(秘密鍵)とする。
5. 秘密鍵で暗号化したデータを本文に付加し、公開鍵で確認することで、本文データを公開したまま、改竄やなりすましを防止する。デジタル署名が可能である(但し、全ての公開鍵がデジタル署名には対応していない)。

【0030】B. 第1の実施形態

以下、本発明の実施形態を、電子スチルカメラに適用した一実施例として、図面を参照して説明する。

【0031】図2は、本発明の第1の実施の形態における電子スチルカメラの構成を示すブロック図である。図において、撮影系1は、レンズを介して結像した静止映像を電気信号に変換するCCD、上記静止映像信号をデジタルデータ(以下、画像データという)に変換するA/D変換器等からなり、画像データをCPUへ供給する。画像記録用メモリ2は、図示しない圧縮/伸張手段により、例えばJPEG (Joint Photographic Coding Experts Group)方式などの圧縮方式により圧縮された、画像データ(輝度信号と色信号)を格納する。画像記録用メモリ2は、交換可能なフラッシュメモリーカードなどのメディアになっている場合もある。

【0032】CPU3は、プログラムを実行することにより、電子スチルカメラ全体の動作を制御する。ROM

5には、CPU3で実行される上記プログラムが格納されている。ワーク用RAM4は、CPU3のワーキングエリアとして用いられる。計時部6は、クロックをカウントすることにより日時を計時し、CPU3に供給する。表示装置7は、液晶表示器からなり、撮影系により撮影した映像や(リアルタイム表示)、画像記録用メモリ2に格納した撮影後の画像データを表示する。

【0033】不揮発メモリ8には、本発明の重要な構成要素を含む情報が格納される。これは、上述したように、画像記録用メモリ2が交換可能になっている場合には、本構成図のように、別ブロックとなっていることが必要である。このセキュリティ処理に関する不揮発メモリ8は、その機器自体に関するセキュリティ情報を保存するセキュリティメモリ8-1と、外部のユーザの公開鍵を管理する公開鍵メモリ8-2とに分かれる。

【0034】セキュリティメモリ8-1には、図3(a)に示すように、自身の機器固有ID、ID画像、機器使用に必要とされるパスワード情報、暗号化する際に用いる暗号化秘密鍵データ、および公開鍵データが格納されている。機器固有IDは、あらかじめ製造時に書き込まれるユニークな値であり、ランダムな値や製造番号等である。ID画像は、ユーザ間のファイル転送/通信において、送信元ユーザを受信ユーザに認識させるために、転送される画像データに添付される。

【0035】ID画像としては、画像で表されるIDとし、例えば、ユーザの顔や、好きなイラスト、趣味に関わる景物などの画像を用いる。ID画像の格納形態としては、転送やメモリ容量の負担の軽減のため、 16×16 や、 32×32 などの小さな画像(サムネイル)に変換して取り扱う。サムネイルに変換するため、元の情報が失われるので、乱数系列の元をたどれないと言う意味でも、サムネイル変換は効果がある。パスワード情報は、セキュリティにかかわる操作や、カメラ操作全体に対して、ユーザ認証を行うためのものである。該セキュリティメモリ8-1のデータは、ユーザが初めてこの機器を所有した場合に記録され、以後は、基本的には書き換えられない。

【0036】公開鍵メモリ8-2は、図3(b)に示すように、画像データを暗号化して送信する相手毎に、その相手にのみ暗号化された画像データを復元できるようにするために、画像データを暗号化する際に用いる公開鍵、ID画像、および相手の機器を特定するための機器IDを格納している。該ID画像は、ユーザ間のファイル転送/通信において、データを送信する際に受信ユーザを選択するために用いられる。これらの公開鍵メモリ8-2の情報は、随時追加更新される。

【0037】また、撮影時の保証データを唯一無二とするために、秘密鍵や、パスワードは、転送不可となっており、メモリ上の格納形式でも、プログラムと組み合わせる暗号化を行い、ハードウェアの分解などによる、

悪意ある情報窃取に対しても強くしていることが望ましい。

【0038】スイッチ部9は、シャッタースイッチ、表示画像送りスイッチ、カーソルキー等から構成され、各スイッチのオン/オフ状態はCPU3により検出される。通信部10は、パソコン等に画像データを転送するインターフェースや、外部機器へ画像データを通信回線を通じて送信するモデムなどの通信手段である。

【0039】C. 第1の実施形態の動作

以下、全体動作を図4ないし図6に示すフローチャートを参照して説明する。

C-1. セキュリティ情報生成処理

機器に電源が投入されると、まず、ステップS10で、初期化が行われ、ステップS12で、セキュリティメモリ8-1の内容を確認し、ステップS14で、初回起動であるかを判断する。初回起動である場合には、機器の使用に先立って、ユーザが、ユーザ独自のセキュリティ情報を生成しなくてはならない。前述したように、RSA暗号系を生成するためには、ID、秘密鍵d、公開鍵e、およびそれらの管理のためのパスワードを生成する必要がある。IDについては、本実施例では、機器固有IDおよびユーザID (ID画像) の2つを組み合わせたものを用いる。

【0040】このように2つのID情報を組み合わせる目的は、機器固有IDを暗号化するための管理を行うことで、たとえ、この発明に関わる全ての処理方法が悪用されて、カメラレベルからの偽造が行われた場合も、機器固有IDに、正当な値であるかの検出を行うというもう1段階のセキュリティを加えられることと、ユーザIDも加えたのは、ユーザ間のファイル転送/通信において、転送された画像データの送信元ユーザが受信ユーザに容易に認識できるという利点のためである。

【0041】機器固有IDは、前述したように、図2に示すセキュリティメモリ8-1に製造時に、あらかじめユニークな値として書き込まれている。さらに、ユーザがユーザIDを生成する。本実施例では、ユーザIDとしてユーザが予め設定した画像 (ID画像: サムネイル、16×16) を用いている。これにより、キー操作による文字列入力を少なくして省くことができ、文字列よりも見た目にわかりやすいIDとなる。

【0042】そして、図4に示すステップS14で、初回起動であると判断されると、まず、ID画像の撮影要求モードになる。ステップS16で、ID画像 (例えば、ユーザの顔や、好きなイラスト、趣味に関わる静物など) を撮影し、所定の圧縮方式により圧縮し、例えば16×16ドットのサムネイル画像とする。

【0043】次に、ステップS18で、ユーザにパスワードを要求する。このパスワードは、セキュリティにかかわる操作や、カメラ操作全体に対して、ユーザ認証を行うためのものである。パスワードに関しては、機器使

用に際して繰り返し入力される必要があるため、IDのように画像入力を使えないので、キーを用いた英数字入力等を必要とする。但し、機器レベルのセキュリティ不要とユーザが判断した場合は、このパスワード設定処理を省略することができる。

【0044】次に、ステップS20で、以下の手順に従って秘密鍵e、公開鍵dを生成する。まず、図1に示すステップA10に従い、大きな2つの異なる素数p、qを乱数生成を行う。このために、

f (機器ID、画像ID) = (p, q)

なる関数fを処理することにより、鍵発生を行う。

【0045】この鍵発生アルゴリズムにおいては、比較的大きな素数の組み合わせを、異なるユーザ間で絶対重ならないように設定する必要があり、入力データに乱数発生機構を用いた素数発生処理を行うのが通常である。数式による疑似乱数発生から素数発生の方法だと、アルゴリズムが明らかになると、同じキーの偽造生成が行い易いので、実際のパソコン上の暗号ソフトウェア等では、キー入力間隔やマウスの座標等々を用いて、ランダム系列の発生源としている。本実施例では、同様に決定論的な課程に促さない乱数系列源として、ID画像そのものを、ランダム系列の発生源としている。

【0046】なお、ID画像は、輝度データそのままで、撮影条件、撮影対象により、値にばらつきがあるので、後述のハッシュ関数をかけるなどして、データブロックごとの値のばらつきを一律に行うなどの処理が必要である。p、qが求まれば、図1のステップA12以降に述べた手順に従って、公開鍵e、秘密鍵dを生成する。

【0047】そして、ステップS22で、ID画像をサムネイル化し、セキュリティメモリ8-1に格納し、ステップS24で、パスワード情報、公開鍵e、秘密鍵dをセキュリティメモリ8-1に格納する。

【0048】C-2. 撮影データ保証情報付加処理
次に、通常の撮影でデジタル署名が付加され、撮影時点データ内容が保証されたファイルが生成される動作に付いて説明する。

【0049】機器に電源が投入された際に、初回起動でない場合には、ステップS14から図5に示すステップS26へ進む。ステップS26では、機器の動作モードがREC (撮影) モード、PLAY (再生) モード、通信モードのいずれであるかを判断する。ここで、RECモードに設定されている。またはRECモードが選択された場合には、ステップS28で、撮影処理を行い、ステップS30で、デジタル署名付加を行った後、画像記録用メモリ2に格納し、ステップS26へ戻る。

【0050】ここで、図7に、ソースとなる画像や日時等の情報をどのようにして、デジタル署名名付のデータファイルとすることを模式的に表している。図示するように、撮影データ本体は、撮影時の日時情報、セキュリテ

ィメモリ8-1に格納されている機器ID、撮影者ID(1D画像)および圧縮済みの画像データからなる。なお、画像データは、撮影時に圧縮されるが、これに限らず、暗号化後に全体を圧縮するようにしてもよい。まず、上記撮影データ本体からハッシュ関数で特徴データを抽出し、次いで、該ダイジェスト化されたデータに対し、秘密鍵で暗号化を施し、電子署名データを生成する。そして、ヘッダ(識別、顔検情報等)・ファイルタイプ(内容証明)、公開鍵(記録者)、上記電子署名データ、および撮影データ本体から最終的なデータファイルを構成する。なお、ダイジェスト化の方法や、暗号系の計算処理については、他の文献に詳しいので省略する。ここでは、自分の公開鍵も、署名確認のための情報として同時に添付している。

【0051】また、ここで特筆すべきなのは、これだけのセキュリティ機構を持ったカメラであっても、自分のデジタル署名を付加できるのは、撮影時だけという事である。他人からの受け取ったデータに対して暗号化されたものであろうと、デジタル署名付きであろうと、それを、この実施例で、あらためてデジタル署名をつけることは不可能になっている。従って、機器ID管理のセキュリティレベルを高くすれば、この機器のIDを持つ画像は、かならず、撮影された画像そのままであるということが自動的に証明される。

【0052】ここで、機器固有IDによるセキュリティ保証について図9を参照して説明する。例えば、65536台の機器を管理する場合を想定する。この場合、機器固有IDを16ビット(ソース)で表し、冗長符号化で、より大きな数値、例えば32ビットの数値の中にランダムにばらまき、32ビットの機器固有IDを生成する。従って、適当に機器固有IDを設定しても、正当な機器固有IDである確率は、 $1/65536$ となる。本実施例では、デジタル署名のチェックと同時に機器IDの正当性をチェックしているので、機器固有IDを模倣することはほぼ不可能である。

【0053】C-3. 画像のデジタル署名チェック、復号化および閲覧

また、機器の動作モードが、PLAY(再生)モードに設定されている。またはPLAY(再生)モードが選択された場合には、ステップS32～ステップS42において、撮影したデータを、セキュリティ付きファイルに関して、閲覧/操作/確認を行う処理が実行される。

【0054】まず、ステップS32で、表示ポイントで指示されるデータファイルを取り出す。次に、ステップS34で、図7のデータファイルの種別領域を参照し、取り出されたデータファイルの種類を判定する。本発明では、様々なセキュリティ機能があるので、それを、ステップS34～ステップS40の処理で行う。

【0055】ここで、デジタル署名付きデータの場合には、ステップS36に進み、図8に示すような処理によ

りチェックを行う。このチェックは、自分が撮影したデータファイル(撮影したものや、過去のデータをカードや、通信を通じて入手したもの)に対してでも、また、メモリカードや通信を通じて外部からやってきた、他人のデータファイルに対しても同様に行われる。

【0056】すなわち、データファイルに添付されている公開鍵を用いて電子署名データを復号化し、ダイジェスト化されたデータを取得する。また、データファイルのデータ本体からハッシュ関数で特徴データを抽出し、ダイジェスト化されたデータを取得する。ここで、データ本体、ヘッダ、署名のいずれでも、データのどこかに改竄、編集等が加えられた場合には、上記双方のデータは一致せず、これに対して、改竄、編集等が加えられていない場合には、上記双方のデータは一致する。また、データ本体から日時情報、機器ID、撮影者ID(1D画像)および画像データをそれぞれ切り出す。

【0057】また、本実施例のデジタル署名付きデータファイルでは、公開鍵情報が付加されているので、ステップS38で、公開鍵を登録した相手に対する暗号化処理を行えるようにするために、必要に応じて、データファイルに添付されている記録者の公開鍵を図2に示す公開鍵メモリ8-2に登録する。

【0058】次に、ステップS42でチェック結果に応じた表示を行う。ステップS36でのチェック結果により、電子署名データから取得したダイジェスト化されたデータとデータ本体から取得したダイジェスト化されたデータとが一致すれば、すなわち整合性がとれていれば、付加情報として、図12(a)に示すように、画像データとともに、内容証明ができていないことを示すメッセージ(「署名チェックOK!」)、認証内容、撮影日や、機器ID、撮影者のID画像を表示する。

【0059】これらの付加情報は、操作により表示のON/OFFができるようになっている。仮に、故意や意図的な編集、またはフォーマット情報の偽造の場合は、図12(b)に示すような表示となる。画像データおよび付加情報は、図8に示すように、そのままの形で保存されているので、それらを表示することは可能であるが、一旦、改竄すると、デジタル署名との一致がとれないため、警告表示となる。また、ファイルとしては、整合性があっても、有り得ない機器固有IDではないか、過去に登録されたIDと不整合はないか(1D画像が同じで、機器固有IDが異なる等)のチェックも行っており、不整合であれば、図12(c)に示すような表示となる。

【0060】一方、ステップS34におけるファイルヘッダの判定により、暗号化ファイルであることがわかると、自分宛の暗号化であれば、自分が公開した公開鍵で暗号化されているはずなので、ステップS40で、図11に示すように、自分の秘密鍵で復号化処理を行う。暗号化ファイルは、その生成については後述するが、ヘッ

ダ(識別、領域情報等)・ファイルタイプ(暗号化)、暗号データ本体(特定の相手宛)、タミーのデータ本体(公開画像データ付加)からなる。暗号化ファイルの復号化処理では、まず、上記暗号化されたデータファイルの暗号データ本体を、自分の秘密鍵で復号化し、ヘッダ、公開鍵、電子署名、データ本体からなるデータファイルを生産する。

【0061】ここで、復号化が成功すれば、暗号化ファイルには、基本的にデジタル署名がつけられているので、そのまま、デジタル署名チェック処理であるステップS36、S38に進む。そして、データファイルに添付された公開鍵による復号化に成功すれば、ステップS42において、図12(d)に示すような付加情報をつけて表示する。

【0062】一方、暗号化されたデータファイルが破壊されたり、途中で少しでも改竄されていた場合には、図11に示すように、秘密鍵による復号化に失敗するので、ステップS36、S38の処理はスキップされる。そして、この場合には、図12(e)に示すような表示となる。本実施例では、図10または図11に示すように、暗号化ファイルの生成時に、タミーのデータ本体部分に、警告情報や宣伝広告を示す公開画像データを埋め込むことを可能にしている(詳細は後述)。図12(e)に示す例では、ファイルが破れているか、自分宛ではない暗号ファイルである旨のメッセージが表示されるとともに、公開画像データが表示される。

【0063】また、通常のセキュリティ保証のない、画像データからフォーマット変換された場合や、編集等を行うとセキュリティ情報を取り去る機能のある画像編集ツールを通った場合などの、セキュリティ情報がない画像データに対しては、直接ステップS42へ進み、図12(c)に示すように、その旨、表示する。データが付加されている分には、日付情報等の付加情報が保証なしで表示される。

【0064】C-4、画像データの暗号化等
上述したステップS42において画像データを表示すると、図6に示すステップS44へ進み、キー操作を判別し、判別したキー操作に応じて、格納画像に対して、暗号化その他の処理を行う。

【0065】ここで、操作/編集キーが操作された場合には、ステップS46へ進み、表示ポインタの移動や、削除、表示画像の送り、戻し操作などの編集処理を行う。なお、詳細は、通常のモニタ付きデジタル電子スチルカメラに準ずるので説明を省略する。

【0066】また、暗号化処理に対するキー操作が行われた場合には、現在表示されている画像に対して、暗号化処理に入る。まず、暗号化するには、送付先相手の公開鍵が必要なので、ステップS43で、公開鍵メモリ8-2に格納されている、他ユーザのID画像の選択画面を表示し(図13を参照)、その中から、画像で送付

先IDを選択する。なお、暗号化として自分に向けて暗号化することも可能である。この場合、メモ리카ードや、通信で誤って秘密の画像データを送ってしまっても、他人には復元することが不可能となる。

【0067】選択が終了すると、公開鍵メモリ8-2から、該IDユーザの公開鍵を取り出し、ステップS50で、図10に示す暗号化処理を行う。すなわち、前述したステップS30で作成したデジタル署名を付加したデータファイルを、上記送付先の相手の公開鍵で暗号化し、暗号化データを生産する。次に、ヘッダ(識別、領域情報等)、上記暗号化データ本体、タミーのデータ本体から新たな(暗号化された)データファイルを生産する。また、必要に応じて、タミーのデータ本体に公開用画像の埋め込みなども行う。図示の例では、データの問い合わせ先の電話番号を画像データで埋め込んでいる。暗号化が終了したデータファイルは、ステップS52で、新たなファイルとして画像記録用メモリ2に格納する。

【0068】C-5、通信処理
また、図5に示すステップS26において、機器の動作モードが、通信モードに設定されている。または選択された場合には、図5に示すステップS54へ進み、通信部10により、図14に示すように、シリアルポートや内蔵モデム等を用いて、他のカメラやパソコンに対してデータファイルを送信(または受信)する。デジタル署名付きのデータファイルの経路には、例えば、インターネット(HTTP、FTPサーバ)21への公開、パソコン22、24、電子スチルカメラ23がある。

【0069】パソコン22では、電子スチルカメラ20からのデジタル署名付きのデータファイルを復元後、画像データに対して編集、改竄が行われ、さらに、電子スチルカメラ25やパソコン26に送信されている。この場合、パソコン25または電子スチルカメラ26では、データファイルに改竄が行われているので、デジタル署名が不一致となり、画像データおよび付加情報を表示することは可能であるが、警告表示となる。また、電子スチルカメラ23では、電子スチルカメラ20から送信された、そのまのデータファイルを受信するので、内容が保証された画像データおよび付加情報が表示される。さらに、パソコン24では、電子スチルカメラ20から送信されたデータファイルに対して何れも操作することなく、電子スチルカメラ27に送信しているが、この場合、電子スチルカメラ23と同様に内容が保証された画像データおよび付加情報が表示される。

【0070】また、暗号化されたデジタル署名付きデータファイルの経路には、例えば、電子スチルカメラ27、パソコン28、29がある。この場合、電子スチルカメラ20では、送信しようとする相手の公開鍵を予め入手し、登録しておく必要がある。言い換えると、暗号化されたデータファイルを受信しようとするユーザは、自身の公開鍵を事前公開しておく必要がある。図示の例

では、電子スチルカメラ27、パソコン29がこれに相当する。

【0071】データファイルは、電子スチルカメラ20で送信先の公開鍵により暗号化され、相手の機器に送信される。電子スチルカメラ27またはパソコン29では、各々、当然、自身の公開鍵で暗号化されたデータファイルを復号化することができるので、内容が保証された画像データおよび追加情報が表示される。これに対して、パソコン28では、自身宛でないデータファイルを復号化することができない。

【0072】なお、本実施例の、署名チェック機能等は、そのまま、パソコン上のビューワソフトとして実現する事ができる。また、このファイルフォーマットでは、簡便な操作性のため、公開鍵をファイルに埋め込む形にしている。しかしながら、あるユーザに関する、最初の公開鍵の登録はセキュリティ上重要なので、公開鍵の交換は、ファイルに埋め込まず、必ず別経路で行うとしてもよい。また、公開鍵自体の正当性を調べるために、指紋鍵 (Key Fingerprint) などの方式を併用する構成にすることも有効である。

【0073】ここで、ハードウェアの分解などによる、悪意ある情報奪取に対するセキュリティ保証について説明する。本実施形態では、セキュリティに関する情報として、図15(a)に示すように、機器固有ID、ID画像、秘密鍵データ、公開鍵データを、セキュリティメモリ8-1に記憶している。仮に、ハードウェアを分解するなどして、図15(b)に示すように、秘密鍵データ、公開鍵データを不法に入手し、乱数系列の取り出し手法が分かっても、サムネール化前のID画像がないので、再生成の偽造複製は不可能である。また、公開鍵データから逆計算により、秘密鍵を偽造複製することは暗号化アルゴリズムからほぼ不可能である。さらに、図15(c)に示すように、機器固有ID、ID画像を不法に入手し、秘密鍵、公開鍵を偽造したとしても、機器固有IDに基づいて、公開鍵の一致、不一致をチェックするので、双方が一致しない限り完全な偽造複製は不可能である。

【0074】第1実施例では、機器に組み込むことで、記録と同時にセキュリティ情報を付加することができる。また、機器にセキュリティコードの付与手段を組み込んだり、ユーザの容易な変更、解析がしにくい利点もある。

【0075】また、第1実施例では、デジタル電子スチルカメラの画像記録時のセキュリティ情報付加としたが、ボイスレコーダ、スキャナ、デジタル動画撮影装置など、デジタルファイルを生産する入力機器一般に適用してもよい。

【0076】D. 第2の実施形態
上述した第1の実施形態は、当業者間の暗号化によるファイル交換や、不特定多数に対するファイル開示におい

て、撮影時点で認証情報を付加するというものであった。これは、画像の証拠性や正当性を保つためには有効であるが、本第2の実施形態では、さらに、複製や部分使用の防止に有効な構成である。

【0077】一方、特に著作権などの保護においては、複製や部分使用を抑制する効果があるものとして、「電子透かし」がある。電子透かしの方法には種々あるが、画像を記録した時点で、電子透かし情報を入れるというのは、デジタル署名等と同じように、実現可能である。これによる効果を、図16に示す。図示の例では、電子スチルカメラ20で、デジタル署名付きデータファイルの画像データに電子透かしとして「02934857367」を挿入し、パソコン22に送信する。ここで、パソコン22において、画像データ部分を取り出し、複製や編集を施し、別ファイルを生じし、インターネットや他の機器に流したとする。そして、この流出したデータファイルを他の電子スチルカメラ23やパソコン24で取り込み、未承認使用の疑いをチェックする。このとき、元のデータファイルの透かし情報と取りこんだデータファイルの透かし情報とが一致すれば、不正使用であることが分かる。このように、デジタル署名付きデータファイルの画像データ部分を抜き出して、不正使用されている場合にも、それが検出できることがわかる。

【0078】単純に電子透かしを併用する方式としては、図7に示す画像データ本体の、画像データに電子透かしを挿入済みのものを使うということであるし、動作フローでいえば、図4に示すステップS30の処理の前に、「電子透かし情報挿入処理」を入れるだけである。

【0079】また、本実施例をデジタル電子スチルカメラに応用した場合の利点として、通常の画像において、パソコンで電子透かしを後付するために、著作権IDの管理会社のようなものが必要であったが、機器に埋め込んだ、図2のセキュリティメモリ8-1の機器ID情報を用いれば、権利IDチェックのシステムが容易になる。

【0080】次に、電子透かしと公開鍵をさらに高度に併用した場合の構成を図17および図18に示す。図17に示す暗号化(透かし処理、電子署名処理)においては、まず、電子署名に用いる情報である公開鍵(指紋鍵でもよい)を透かし情報として圧縮済みの画像データに入れ込む。次に、該画像データ(圧縮済み、透かし処理済み)に、日時情報、機器ID、撮影者ID(ID画像)を付加し、撮影データ本体とする。そして、該撮影データ本体をダイジェスト化されたデータに対して、秘密鍵で暗号化することにより、電子署名データを生成する。さらに、ヘッダ(識別、領域情報等)・ファイルタイプ(内容証明)、公開鍵、電子署名データおよび撮影データ本体から最終的なデータファイルを生産する。

【0081】図18に示す復号化においては、まず、データファイルに添付されている公開鍵を用いて電子署名

データを復号化し、ダイジェスト化されたデータを取得する。また、データファイルのデータ本体からハッシュ関数等で特徴データを抽出し、ダイジェスト化されたデータを取得し、上記復元されたダイジェスト化されたデータと比較する。ここで、データ本体、ヘッダ、署名のいずれでも、データのどこかに改竄、編集等が加えられた場合には、上記双方のデータは一致せず、これに対して、改竄、編集等が加えられている場合には、上記双方のデータは一致する。また、データ本体の画像データから取り出した透かし情報から公開鍵を取り出し、上記データファイルに添付されている公開鍵と比較し、電子透かし内容の整合性のチェックを行う。そして、それぞれの比較結果が両方とも成立していれば、偽造、改竄のいずれもが行われていないことになる。

【0082】このように、撮影データ本体を付加すること、電子署名のチェックと、電子透かし内容の整合性のチェックを行うことができる。この場合、偽造、改竄を行うには、公開鍵暗号を破るとともに、電子透かしの除去と再挿入のプロセスが必要になり、内容保証のセキュリティレベルをさらに向上させることが可能になる。

【0083】
【発明の効果】請求項1記載の発明によれば、入力手段から入力したデジタルデータに対し、付加情報生成手段により、該デジタルデータに関する付加情報を添付し、入力データ本体として記憶手段に記憶し、電子署名手段により、鍵生成手段より生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成し、ファイル生成手段により、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、およびデータファイルに関する公開可能な公開情報をまとめ、最終的な閲覧ファイルを生成するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0084】また、請求項2記載の発明によれば、復号化手段により、閲覧ファイルに付加されている公開鍵により、閲覧ファイルに添付されている電子署名データを復号化し、判断手段により、前記閲覧ファイルに添付されている入力データ本体と前記復号化手段により復元されたデータとを比較し、双方が一致した場合には、入力データ本体が改竄されていないと判断し、双方が一致しない場合には、入力データ本体が改竄されていると判断し、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記判断手段による判断結果を表示手段に表示するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0085】また、請求項3記載の発明によれば、前記入力データ本体が暗号化される前段で、特徴データ抽出

手段により、入力データ本体から特徴データを抽出し、ダイジェスト化しておき、電子署名データを生成する際には、前記電子署名手段により、前記特徴データ抽出手段によりダイジェスト化されたデータと、前記鍵生成手段により生成された秘密鍵により暗号化するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0086】また、請求項4記載の発明によれば、公開鍵および秘密鍵をデジタルデータの記録者を識別するための識別データに基づいて生成するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0087】また、請求項5記載の発明によれば、前記識別データを、デジタルデータの記録者が選択した任意の識別画像データとしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0088】また、請求項6記載の発明によれば、開引き手段により、識別画像データを所定のサイズに開引き、該開引かれた識別画像データを前記入力手段から入力されたデジタルデータに付加情報として添付するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0089】また、請求項7記載の発明によれば、配信相手毎に、配信相手を選定する識別情報として、配信相手によって予め設定された識別画像データを配信相手情報記憶手段に記憶しておき、配信先選択手段により、識別画像データを指定することで、閲覧ファイルの配信相手を選択するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0090】また、請求項8記載の発明によれば、配信相手毎に、配信相手を選定する識別情報として、配信相手によって予め設定された識別画像データと、配信相手によって予め配信された公開鍵とを配信相手情報記憶手段に記憶しておき、暗号化手段により、前記電子署名生成手段より生成された電子署名データと、前記配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化し、前記閲覧ファイル生成手段により、前記暗号化手段により暗号化された暗号データおよび公開可能な公開情報をまとめ、閲覧ファイルを生成するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0091】また、請求項9記載の発明によれば、前記公開情報を、少なくとも、公開可能な画像データとしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0092】また、請求項10記載の発明によれば、第2の復号化手段により、前記閲覧ファイルを自身の秘密鍵により復号化した後、前記復号化手段により、前記第

2の復号化手段により復元されたデータに添付されている公開鍵で、復元されたデータに添付されている電子署名データを復号化するようにしたので、デジタルデータの改竄や複製、部分使用を防止することができるという利点が得られる。

【0093】また、請求項1記載の発明によれば、前記第2の復号化手段による復元が失敗した場合には、前記開鍵手段により前記閲覧ファイルが不正に入手されたと判断し、前記閲覧ファイルに添付されている入力データ本体のデジタルデータとともに、前記公開情報に含まれる公開可能な画像データを表示手段に表示するようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【0094】また、請求項1記載の発明によれば、前記公開情報を、閲覧ファイルに添付されているデータ本体が暗号化ファイル、電子署名付きファイル、セキュリティ情報なしファイルのいずれであるかを示すファイル種別情報としたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【0095】また、請求項13記載の発明によれば、前記電子署名手段による電子署名データの生成に先立って、電子透かし手段により、前記入力手段から入力されたデジタルデータに、前記鍵生成手段により生成された公開鍵を電子透かし情報として入れ込むようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【0096】また、請求項14記載の発明によれば、前記閲覧ファイルに付加されている公開鍵と、前記閲覧ファイルのデータ本体に電子透かし情報として入れ込まれた公開鍵とを比較し、双方が一致した場合には、入力データ本体が正当な配信者からのデータであると判断するようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【0097】また、請求項15記載の発明によれば、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、入力手段から入力されたデジタルデータに対し、付加情報生成手段により、該デジタルデータに関する付加情報を添付し、入力データ本体として記憶手段に記憶し、電子署名手段により、鍵生成手段により生成された秘密鍵で、前記記憶手段に記憶された入力データ本体を暗号化して電子署名データを生成し、いったん、第1の閲覧ファイル生成手段により、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめて閲覧ファイルを生じ、次いで、該閲覧ファイルを、暗号化手段により、配信相手情報記憶手段に記憶されている、配信相手の公開鍵により暗号化

し、さらに、第2の閲覧ファイル生成手段により、ファイル本体の種別を示すファイル種別情報、前記暗号化手段により暗号化された暗号データ、および公開可能な公開画像データをまとめて最終的な閲覧ファイルを生じするようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【0098】また、請求項16記載の発明によれば、公開鍵暗号方式により公開鍵および秘密鍵を生成する鍵生成手段と、入力手段から入力されたデジタルデータに対し、電子透かし手段により、鍵生成手段で生成された公開鍵を電子透かし情報として入れ込み、付加情報生成手段により、該デジタルデータに関する付加情報を添付し、入力データ本体として記憶手段に記憶し、次いで、電子署名手段により、鍵生成手段により生成された秘密鍵により、前記記憶手段に記憶された入力データ本体を暗号化し、電子署名データを生成し、閲覧ファイル生成手段により、前記記憶手段に記憶された入力データ本体、前記電子署名手段により生成された電子署名データ、前記鍵生成手段により生成された公開鍵、および本データファイルに関する公開可能な公開情報をまとめて、閲覧ファイルを生じするようにしたので、デジタルデータの改竄や複製、部分使用、不正使用を防止することができるという利点が得られる。

【図面の簡単な説明】

【図1】RSA公開鍵暗号方式を説明するためのフローチャートである。

【図2】本発明の第1の実施態様における電子スチルカメラの構成を示すブロック図である。

【図3】不揮発性メモリ8のデータ構成を示す概念図である。

【図4】電子スチルカメラの動作を説明するためのフローチャートである。

【図5】電子スチルカメラの動作を説明するためのフローチャートである。

【図6】電子スチルカメラの動作を説明するためのフローチャートである。

【図7】電子署名付きのデータファイルの生成方法を説明するための概念図である。

【図8】電子署名付きのデータファイルの復元方法を説明するための概念図である。

【図9】機器固有IDによるセキュリティ保証を説明するための概念図である。

【図10】暗号化方法を説明するための概念図である。

【図11】暗号化された電子署名付きのデータファイルの復元方法を説明するための概念図である。

【図12】表示例を示す概念図である。

【図13】ID画像の例を示す概念図である。

【図14】データファイルの送信経路を説明するための概念図である。

【図15】情報奪取に対するセキュリティ保証を説明するための概念図である。

【図16】本発明の第2の実施形態による電子透かしを適用した場合の概念図である。

【図17】電子透かしを適用した場合の電子署名付きデータファイルの生成方法を説明するための概念図である。

【図18】電子透かしを適用した場合の電子署名付きデータファイルの復元方法を説明するための概念図である。

【符号の説明】

1 撮影系

2 画像記録用メモリ

3 CPU

4 ワーク用RAM

5 ROM

6 計時部

7 表示装置

8 不揮発メモリ

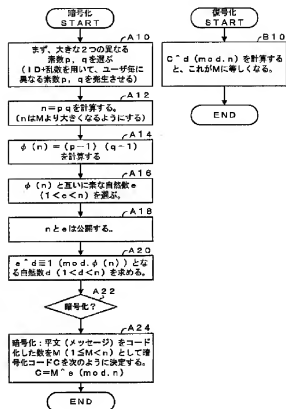
8-1 セキュリティメモリ

8-2 公開鍵メモリ

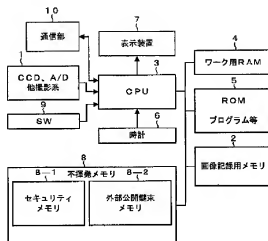
9 スイッチ部

10 通信部

【図1】



【図2】



【図3】

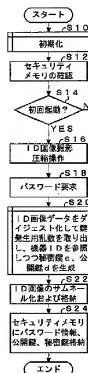
(a)

秘密固有ID
ID固有サムネールデータ (10×16) 等
パスワード情報
秘密鍵データ
公開鍵データ

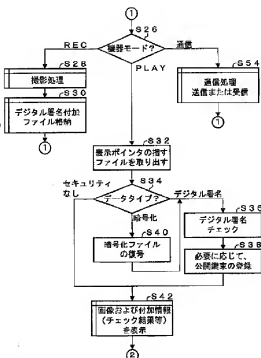
(b)

インデックス情報
ユーザA
ユーザB
ユーザC
ユーザD
ユーザE
ユーザF
ユーザG
ユーザH
ユーザI
ユーザJ
ユーザK
ユーザL
ユーザM
ユーザN
ユーザO
ユーザP
ユーザQ
ユーザR
ユーザS
ユーザT
ユーザU
ユーザV
ユーザW
ユーザX
ユーザY
ユーザZ

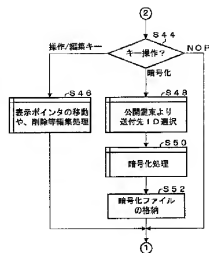
【図4】



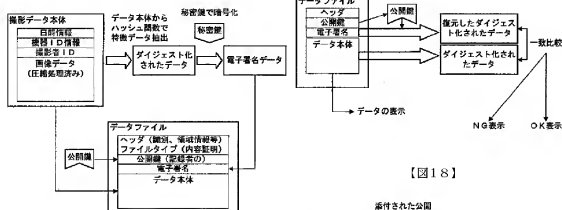
【図5】



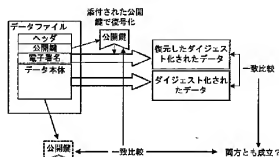
【図6】



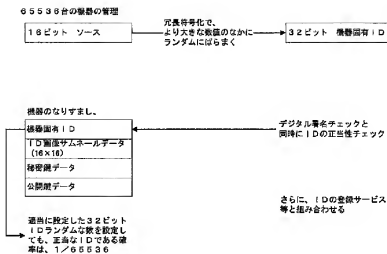
【図7】



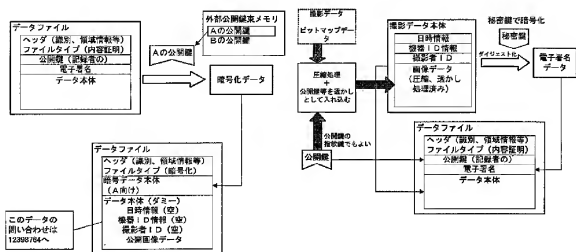
【図18】



【図9】



【図10】

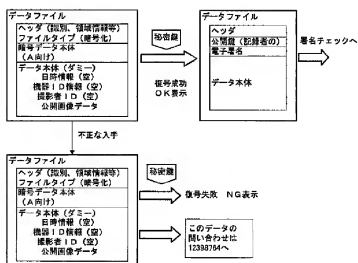


【図13】



画像ID選択による
暗号化時の送付先指定

【図11】



【図12】

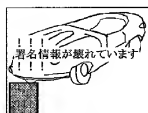
(a)



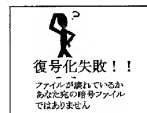
(d)



(b)



(e)

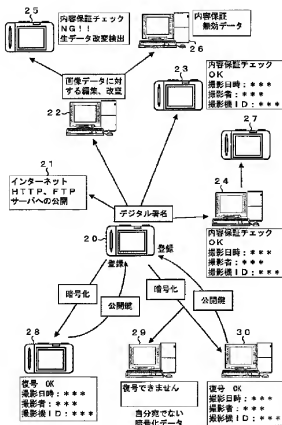


(c)

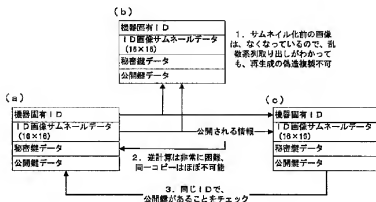


暗号化ファイルの
公開部に含まれている画像

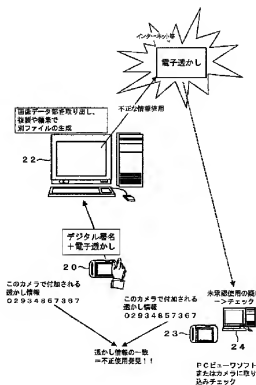
【图 14】



【图15】



【例 16】



フロントページの続き